AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A cryptographic system ~~combining the so called discrete logarithm and factorization principles,~~ comprising at least one of an encryption system and a decryption system that utilizes~~, among other things,~~ public keys and a secret key, wherein ~~the~~ said public keys comprise, at least:

a. an RSA modulus n, greater in size than 640 bits, having the following property:

$n = (A\ p_A + 1) \times (B\ p_B + 1)$

in which:

p_A and p_B are prime numbers greater in size than 320 bits,

$(A\ p_A + 1)$ is an RSA prime denoted p,

$(B\ p_B + 1)$ is an RSA prime denoted q,

A is the product of k/2 (k being an even integer number between 10 and 120) prime numbers (denoted p[i], i = 1 to k/2) of relatively small size (between 2 and 16 bits) and

B is the product of k/2 prime numbers (also denoted p[i], i = k/2 + 1 to k);

the p[i]s being of relatively small size (between 2 and 16 bits), and also able to be mutually prime;

b. an exponentiation base g, of order $\Phi(n)/4$ (where $\Phi(n)$ denotes the Euler indicator function), g therefore having not to be a p[i]-th power modulo n of any number.

2. (Currently Amended) A cryptographic system according to Claim 1 comprising at least an encryption/decryption system[[1]], wherein the encryption of a message m, m < AB, ~~consists of~~ comprises the operation:

$$c = g^m \bmod n$$

where c denotes the cryptograph (encrypted message).

3. (Currently Amended) A cryptographic system according to Claim 2 comprising an encryption/decryption system, wherein the integrity of a message m can be provided by the encryption of m|h(m) (h denoting a hashing function and | denoting concatenation), or by the encryption of DES (key, m), ~~the~~ where said key ~~being~~ is a key accessible to all.

4. (Currently Amended) A cryptographic system according to Claim 1 comprising an encryption/decryption system, and a key escrow system, wherein the ~~said~~ secret key of ~~the~~ a decrypter or of ~~the~~ an escrow ~~centre~~ authority is the number Φ(n), and ~~in that~~ wherein the operation of decryption or of recovering the identity of a user ~~consists of~~ comprises the following steps:

a. calculating, for i from 1 to k: $y[i] = c^{\Phi(n)/p[i]} \bmod n$;

b. for i from 1 to k

for j from 1 to p[i]

comparing y[i] with the values $g^{j\Phi(n)/p[i]} \bmod n$ independent of m;

if $g^{j\Phi(n)/p[i]} \bmod n = y[i]$ then assign $\mu[i] = j$

c. reconstructing ~~the~~ a message m from the Chinese remainder theorem CRT and the values μ[i].

5. (Currently Amended) A cryptographic system according to Claim 4 ~~or 5~~ comprising an encryption/decryption system and a key escrow system, ~~the~~ wherein said decrypter speeds up the calculation of the quantities y[i] by calculating:

a) $z = c^r \bmod n$ where $r = p_A p_B$

b) for i from 1 to k: $y[i] = z^{AB/p[i]} \bmod n$,

so as to take advantage of the difference in size between AB/p[i] and $\Phi(n)/p[i]$ for speeding up the calculations.

6. (Currently Amended) A cryptographic system according to Claim 4 comprising an encryption/decryption system and a key escrow system ~~or 5~~, wherein the decrypter pre-calculates and saves, once and for all, the table of values $g^{j\Phi(n)/p[i]} \bmod n$ for $1 \leq i \leq k$ and $1 \leq j \leq p[i]$

or,

~~more specifically,~~ a truncation or a hashing of these values (denoted h) having the following property:

$h(g^{j\Phi(n)/p[i]} \bmod n) \neq h(g^{j'\Phi(n)/p[i]} \bmod n)$ if $j \neq j'$.

7. (Currently Amended) A cryptographic system according to any one of ~~Claim~~ Claims 4 to 6 comprising an encryption/decryption system and a key escrow system, wherein the decrypter speeds up its calculations by separately decrypting the message modulo p and then modulo q, and constructing the modulo results with the help of the Chinese remainder theorem in order to find m again.

8. (Currently Amended) A cryptographic system according to ~~any one of Claims 4 to 7~~ Claim 4, wherein a key escrow ~~centre or~~ authority ~~implemented~~ implements the following steps:

a. it codes the identify of the user $ID = \Sigma\ 2^{i-1}\ ID[i]$ where ID[i] are the bits of the identity of the said user of the system (the sum being taken for I from 1 to k) by calculating $e(ID) = \pi\ p[i]^{ID(i)}$ (the product being taken for I from 1 to k);

b. it issues, to the user, an El-Gamal key (that is to say an exponentiation base) $c = g^{e(ID)u} \bmod n$,

in which u is a large random prime or a number prime with $\Phi(n)$;

c. it thus makes it possible for the user to derive, from c, his El-Gamal public key by choosing a random number x and raising c to the power x ~~modulo n.~~ modulo n;

d. with the aim of finding the trace of the user, the authority extracts, from ~~the~~ an El-Gamal cryptogram of ~~the~~ an encrypter, ~~the~~ said cryptogram always comprising two parts, the part:

$v = c^r \bmod n$

where r is the encryption random number chosen by the ~~encrypter.~~ encrypter;

e. knowing $\Phi(n)$, ~~the~~ said authority finds the bits ID[i] by means of the following algorithm:

1. calculate, for i from 1 to k: $y[i] = v^{\Phi(n)/p[i]} \bmod n$

2. if $y[i] = 1$, then $\mu[i] = 1$, otherwise $\mu[i] = 0$

3. calculate:

   $ID' = \Sigma\ 2^{i-1}\ \mu[i]$

4. find: ID = CCE(ID')

in which CCE denotes an error correction mechanism.

9. (Currently Amended) A cryptographic system according to ~~any one of Claims 4 to 7~~ Claim 4 comprising a key escrow system, ~~it is~~ based on ~~the so-called~~ a Diffie-Hellman key exchange mechanism where a number c, obtained by raising g to a random power a modulo n by one ~~of the parties~~ party, is intercepted by ~~the~~ said escrow authority:

$c = g^a \bmod n$

~~the~~ said escrow authority finds a again in the following manner:

a. knowing the factorization of n, ~~the~~ said authority finds, with the help of the decryption algorithm, the value

$\alpha = a \bmod AB$

that is $a = \alpha + \beta AB$;

b. ~~the~~ said authority calculates: $\lambda = c/g^\alpha \bmod n = g^{\beta AB} \bmod n$

c. using a cryptanalysis algorithm, the authority calculates the discrete logarithm β

$\lambda = (g^{AB})^\beta \bmod n$

d. the authority finds

$a = \alpha + \beta AB$

and decrypts the communications based on the use of a.

10. A cryptographic system according to ~~any one of Claims 2 to 9~~ Claim 2 comprising an encryption/decryption system and a key escrow system, wherein the RSA modulus n is the product of three factors:

$n = (Ap_A + 1) \times (Bp_B + 1) \times (Cp_c + 1)$

in which p_A, p_B, p_C are prime numbers greater in size than 320 bits,

$(Ap_A + 1)$, $(Bp_B + 1)$, $(Cp_c + 1)$ are RSA primes, denoted respectively p, q, r,

A, B and C are each the product of k/3 prime numbers (denoted p[i], i = 1 to k), the p[i]s being of relatively small size (between 2 and 16 bits) and able to be mutually prime numbers and k being an integer number between 10 and 120, so that the product ABC has at least 160 bits.

Claims 11-12. (Canceled)

13. (Currently Amended) A cryptographic system ~~wherein~~ including at least one of an encryption system and a decryption system that uses a public key and a private key ~~are used~~ in providing secure encryption and decryption of a message m, the public key comprising:

an RSA modulus n, wherein n is greater than 640 bits, and wherein $n = (Ap_A + 1)(Bp_B + 1)$, wherein p_A and p_B are prime numbers greater in size than 320 bits, $(Ap_A + 1)$ is an RSA prime denoted p, $(Bp_B + 1)$ is an RSA prime denoted q, A is the product of k/2 prime numbers p[i], i = 1 to k/2, B is the product of k/2 prime numbers p[i], i = 1 to k/2, the p[i]'s being mutually prime, and wherein k is an even integer; and

an exponentiation base g, wherein g is of the order $\Phi(n)/4$, $\Phi(n)$ being the Euler indicator function.

14. (Previously Presented) The cryptographic system of claim 13, wherein the message m is encrypted into a cryptogram c according to $c = g^m \bmod n$.

15. (Currently Amended) The cryptographic system of claim 14, wherein the integrity of the message m can be provided by the encryption $m|h(m)$ wherein h(m) is a hashing function and | ~~denoting~~ denotes concatenation.

16. (Previously Presented) The cryptographic system of claim 14, wherein the integrity of the message m can be provided by the encryption of a DES key, wherein the DES key is publicly available.

17. (Previously Presented) The cryptographic system of claim 13, wherein the secret key is equal to $\Phi(n)$, and wherein decryption of the message m according to reconstructing the message m from the Chinese remainder theorem CRT and the values $\mu[i]$, where $\mu[i] = j$ when $g^{j\Phi(n)/p[i]} \bmod n = y[i]$, $y[i] = c^{\Phi(n)/p[i]} \bmod n$.

18. (Currently Amended) The cryptographic system of claim 17, wherein the decrypter speeds up its calculations by separately decrypting the ~~messgae~~ message modulo p and then modulo q, and constructing the modulo results with the help of the Chinese remainder theorem to obtain the message m.

19. (Previously Presented) The cryptographic system of claim 17, further comprising:

an El-Gamal key $c=g^{e(ID)u} \bmod n$, wherein u is a large random prime, $ID = \Sigma 2^{i-1} ID[i]$, ID[i] representing bits of the identity of a user of the system.

20. (Previously Presented) A method of encrypting a message m, comprising:

calculating n according to $n = (Ap_A + 1)(Bp_B + 1)$, wherein p_A and p_B are prime numbers greater in size than 320 bits, $(Ap_A + 1)$ is an RSA prime denoted p, $(Bp_B + 1)$ is an RSA prime denoted q, A is the product of k/2 prime numbers p[i], i = 1 to k/2, B is the product of k/2 prime numbers p[i], i = 1 to k/2, the p[i]'s being mutually prime, and wherein k is an even integer; and

calculating a cryptogram of the message m according to $c = g^m \bmod n$, wherein the exponentiation base g is of the order $\Phi(n)/4$, $\Phi(n)$ being the Euler indicator function.

21. (Previously Presented) The method of claim 20, wherein the message m is decrypted, further comprising:

calculating for i = 1 to k: $y[i] = c^{\Phi(n)/p[i]} \bmod n$;

comparing y[i] with values $g^{j\Phi(n)/p[i]} \bmod n$ independent of m, for I from 1 to k and j from 1 to p[i];

if $g^{j\Phi(n)/p[i]} \bmod n = y[i]$ then assign $\mu[i] = j$; and

reconstructing the message m from the Chinese remainder theorem CRT and the values $\mu[i]$.

22. (Previously Presented) The method of claim 21, wherein the decrypter speeds up the calculation of the quantities $y[i] = z^{AB/p[i]}$ by calculating $z = c^r \bmod n$ where $r = p_A p_B$ for = 1 to k.

23. (Previously Presented) The method of claim 21, wherein the decrypter calculates and saves the table of values $g^{j\Phi(n)/p[i]}$ mod n for i from 1 to k and j for 1 to p[i].